

## PATENT COOPERATION TREATY

PCT

## NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Commissioner  
 US Department of Commerce  
 United States Patent and Trademark  
 Office, PCT  
 2011 South Clark Place Room  
 CP2/5C24  
 Arlington, VA 22202  
 ETATS-UNIS D'AMERIQUE  
 in its capacity as elected Office

Date of mailing (day/month/year)  
 19 March 2001 (19.03.01)

International application No.  
 PCT/SE00/01407

Applicant's or agent's file reference  
 56087-60575

International filing date (day/month/year)  
 03 July 2000 (03.07.00)

Priority date (day/month/year)  
 01 July 1999 (01.07.99)

Applicant

GÜNDNER, Hans, Martin et al

1. The designated Office is hereby notified of its election made:



in the demand filed with the International Preliminary Examining Authority on:

25 January 2001 (25.01.01)



in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was

was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO  
 34, chemin des Colombettes  
 1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Claudio Borton

Telephone No.: (41-22) 338.83.38

BEST AVAILABLE COPY

PCT

NOTIFICATION OF THE RECORDING  
OF A CHANGE

(PCT Rule 92bis.1 and  
Administrative Instructions, Section 422)

From the INTERNATIONAL BUREAU

To:

ALBIHNS STOCKHOLM AB  
Box 5581  
S-114 85  
Stockholm  
SUÈDE

Date of mailing (day/month/year) 20 December 2001 (20.12.01)
Applicant's or agent's file reference 56087-60575
International application No. PCT/SE00/01407

IMPORTANT NOTIFICATION
International filing date (day/month/year) 03 July 2000 (03.07.00)

BEST AVAILABLE COPY

1. The following indications appeared on record concerning: <input checked="" type="checkbox"/> the applicant <input type="checkbox"/> the inventor <input type="checkbox"/> the agent <input type="checkbox"/> the common representative		
Name and Address SIKE & CO Gjuterigatan 3 A S-553 18 Jönköping Sweden	State of Nationality SE	State of Residence SE
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	
2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning: <input checked="" type="checkbox"/> the person <input type="checkbox"/> the name <input type="checkbox"/> the address <input type="checkbox"/> the nationality <input type="checkbox"/> the residence		
Name and Address IUC SJUHARAD AB Nyboholm S-523 37 Ulricehamn Sweden	State of Nationality SE	State of Residence SE
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	
3. Further observations, if necessary:		
4. A copy of this notification has been sent to: <input checked="" type="checkbox"/> the receiving Office <input type="checkbox"/> the designated Offices concerned <input type="checkbox"/> the International Searching Authority <input checked="" type="checkbox"/> the elected Offices concerned <input type="checkbox"/> the International Preliminary Examining Authority <input type="checkbox"/> other:		

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer Jean-Marie MCADAMS Telephone No.: (41-22) 338.83.38
---	--

## PATENT COOPERATION TREATY

PCT

From the INTERNATIONAL BUREAU

NOTIFICATION OF THE RECORDING  
OF A CHANGE(PCT Rule 92bis.1 and  
Administrative Instructions, Section 422)

To:

ALBIHNS PATENTBYRÅ AB  
Box 5581  
S-114 85 Stockholm  
SUÈDEDate of mailing (day/month/year)  
29 March 2001 (29.03.01)Applicant's or agent's file reference  
56087-60575

## IMPORTANT NOTIFICATION

International application No.  
PCT/SE00/01407International filing date (day/month/year)  
03 July 2000 (03.07.00)

BEST AVAILABLE COPY

1. The following indications appeared on record concerning:

☐ the applicant ☐ the inventor ☒ the agent ☐ the common representative

Name and Address

ALBIHNS PATENTBYRÅ STOCKHOLM AB  
Box 5581  
S-114 85 Stockholm  
Sweden

State of Nationality

State of Residence

Telephone No.

+46 8 59 88 72 00

Facsimile No.

+46 8 59 88 73 00

Teleprinter No.

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☐ the person ☒ the name ☐ the address ☐ the nationality ☐ the residence

Name and Address

ALBIHNS PATENTBYRÅ AB  
Box 5581  
S-114 85 Stockholm  
Sweden

State of Nationality

State of Residence

Telephone No.

+46 8 59 88 72 00

Facsimile No.

+46 8 59 88 73 00

Teleprinter No.

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

☒ the receiving Office ☐ the designated Offices concerned  
☐ the International Searching Authority ☒ the elected Offices concerned  
☒ the International Preliminary Examining Authority ☐ other:The International Bureau of WIPO  
34, chemin des Colombettes  
1211 Geneva 20, Switzerland

Authorized officer

Jean-Marie McAdams

Facsimile No.: (41-22) 740.14.35

Telephone No.: (41-22) 338.83.38

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 00/01407

## A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G08F 13/14

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G08B, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9703397 A1 (BENKTA CONSULTING AB), 30 January 1997 (30.01.97), page 1, line 34 - page 2, line 17; page 3, line 7 - page 4, line 16	1,3-8,11
Y	--	2,9
X	US 5406261 A (J.T.GLENN), 11 April 1995 (11.04.95), column 4, line 16 - line 36; column 5, line 50 - column 6, line 7; column 7, line 21 - line 47, figures 4,5	11
Y	--	2,9

☒ Further documents are listed in the continuation of Box C.☒ See patent family annex.

- \* Special categories of cited documents
- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

7 October 2000

Date of mailing of the international search report

17-10-2000

Name and mailing address of the ISA/  
Swedish Patent Office  
Box 5055, S-102 42 STOCKHOLM  
Facsimile No. +46 8 666 02 86

Authorized officer

Gunnel Wästerlid/itw  
Telephone No. +46 8 782 25 00

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 00/01407

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5767771 A (L.A.LAMONT), 16 June 1998 (16.06.98), column 3, line 40 - column 4, line 57; column 5, line 29 - line 52, figure 6  --	1,3-8,11
Y	GB 2300508 A (DERITEND ELECTRO-MECHANICAL SERVICES LTD.), 16 November 1996 (16.11.96), page 1, line 38 - page 2, line 14; page 4, line 28 - page 5, line 21; page 6, line 4 - line 21, abstract, p.7,1.5-p.8,1.12,p.9, 1.26-1.33  --	1,3-8,11
A	US 5760690 A (R.A.FRENCH), 2 June 1998 (02.06.98), column 1, line 57 - column 2, line 21  -- -----	1-11

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

01/08/00

International application No.  
PCT/SE 00/01407

Patent document cited in search report			Publication date	Patent family member(s)		Publication date
WO	9703397	A1	30/01/97	SE	9502537 A	11/01/97
US	5406261	A	11/04/95	NONE		
US	5767771	A	16/06/98	NONE		
GB	2300508	A	16/11/96	AU	2529495 A	21/11/96
				GB	2300743 A	13/11/96
				GB	9508716 D	00/00/00
				GB	9514679 D	00/00/00
				WO	9635195 A	07/11/96
US	5760690	A	02/06/98	NONE		

# PATENT COOPERATION TREATY

## PCT

### INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

REC'D 31 OCT 2001

14

Applicant's or agent's file reference 56087-60575	<b>FOR FURTHER ACTION</b>	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/SE00/01407	International filing date (day/month/year) 03-07-2000	Priority date (day/month/year) 01-07-1999
International Patent Classification (IPC) or national classification and IPC <sub>7</sub> G08B 13/14		
Applicant SIKE & CO et al		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of \_\_\_\_\_ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand  25-01-2001	Date of completion of this report  24-10-2001
Name and mailing address of the IPEA/SE Patent- och registreringsverket Box 5055 S-102 42 STOCKHOLM Facsimile No. 08-667 72 88	Authorized officer  Gordana Nincovic' /itw Telephone No. 08-782 25 00

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/SE00/01407

## I. Basis of the report

1. With regard to the **elements** of the international application:\*

- ☒ the international application as originally filed
- ☐ the description:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the claims:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, as amended (together with any statement) under article 19  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the drawings:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the sequence listing part of the description:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language \_\_\_\_\_ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages \_\_\_\_\_
- ☐ the claims, Nos. \_\_\_\_\_
- ☐ the drawings, sheet/fig \_\_\_\_\_

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2 (c)).\*\*

\* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).

\*\* Any replacement sheet containing such amendments must be referred to under item I and annexed to this report.



## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/SE00/01407

**V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement****1. Statement**

Novelty (N)	Claims	<u>1-11</u>	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	<u>1-11</u>	NO
Industrial applicability (IA)	Claims	<u>1-11</u>	YES
	Claims		NO

**2. Citations and explanations (Rule 70.7)**

The present invention relates to a method and an apparatus for preventing electrical equipment from theft, such as components in a computer, comprising an internal sensor arrangement, in connection with a control means, for monitoring whether an unauthorised person has opened a housing of the equipment and an identification means for identifying authorised users. Unauthorised opening of the housing results in activation of a destruction means with an electric pulse fed through the electronic components, whereby the components are irreversibly set out of order.

Documents cited in the International Search Report:

D1 WO 97/03397 A1 (Benkta Consulting AB), 30.01.97  
D2 US 5406261 A (J.T. Glenn), 11.04.95  
D3 US 5767771 A (L.A. Lamont), 16.06.98  
D4 GB 2300508 A (Deritend el-mech. services LTD), 16.11.96  
D5 US 5760690 A (R.A. French), 02.06.98

Document D1 discloses an arrangement and a method for deterring the theft of computers and computer components comprising a number of sensing means for detecting improper manipulation of computer or its components, whereby an internal logic unit cause a destruction means to trigger a shock signal directed to vital components of the computer so as to partially or completely destroy them. The arrangement is provided with a batteries, capacitors or the like connected to voltage generator means for generating a shock voltage signal and also a code panel including a device in the form of remote control unit having a keyboard through which the code signal can be entered and an authorised person can disconnect the security arrangement. (See page 1, line 34 - page 2, line 17; page 3, line 7 - page 4, line 16). ... / ...

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/SE00/01407

**Supplemental Box**

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: V

Document D2 discloses an arrangement and a method for preventing theft and unauthorised access to a computer system and generating an alarm signal. A motion sensor can be used to detect if the computer is being tampered with and for highly sensitive data a destruction means can be installed that would unrecoverably destroy vital components by using a high voltage or a chemically reactive device, such as a microexplosive charge or acid. The arrangement comprises also a wireless remote control means in connection with a corresponding receiver that controls various functions e.g. activating and deactivating the alarm, arming and disarming the destruction means etc. An authorised user can be identified using a coded signal, a voice detector or a finger print reader decoder. (See column 4, line 16 - line 36; column 5, line 50 - column 6, line 7; column 7, line 21 - 47).

Document D3 discloses also an electronic equipment theft deterrent system which disables vital components of electronic equipment in response to the unauthorised tampering, comprising a sensor means to detect unauthorised removal and a disabling circuit having a high voltage output connected to components in order to permanently destroy them. The theft deterrent circuit can also be armed remotely. An authorised user is permitted access to the equipment by a unique code. (See column 3, line 40 - column 4, line 57; column 5, line 29 - 52).

Document D4 discloses a security alarm device for computer capable to be built into one of the standard components of the computer, comprising means for detecting movement of the computer and means for detecting tampering with the computer. A control element is arranged to raise an alarm if movement or tampering is detected and furthermore the device may be arranged to disable the computer to make it worthless to the thief. (See page 1, line 38 -page 2, line 14; page 4, line 28 - page 5, line 21; page 6, line 4 - 21; page 7, line 5 - page 8, line 12; page 9, line 26 - 33).

Document D5 discloses a portable computer with integrated alarm system.

... / ...

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/SE00/01407

**Supplemental Box**

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: V

What is defined in claims 1 and 11 does not differ from the known technique described in documents D1 - D4 in any essential way, see specially document D1. To use an internal sensor instead of external, as it is described in document D1, is already known from document D4, which implied that an alarm device for computer can be built into one of the standard components of the computer. Therefore the invention according to claims 1 and 11 is considered obvious to a person skilled in the art. Accordingly, the invention according to these claims is not considered to involve an inventive step.

In view of the cited documents, remaining claims are matters of fact which are previously known from cited documents or are obvious to a person skilled in the art. Therefore the subject matter of these claims is not considered to involve an inventive step.

The claimed invention is regarded to be industrially applicable.

PCT

NOTICE INFORMING THE APPLICANT OF THE  
COMMUNICATION OF THE INTERNATIONAL  
APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

From the INTERNATIONAL BUREAU

To:

ALBIHNS PATENTBYRÅ STOCKHOLM AB  
Box 5581  
S-114 85 Stockholm  
SUÈDE

Besv

001	01	01	19
001	01	01	19
001	01	01	19
001	01	01	19

IMPORTANT NOTICE

Date of mailing (day/month/year) 11 January 2001 (11.01.01)		
Applicant's or agent's file reference 56087-60575		
International application No. PCT/SE00/01407	International filing date (day/month/year) 03 July 2000 (03.07.00)	Priority date (day/month/year) 01 July 1999 (01.07.99)
Applicant SIKE & CO et al		

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:

AG,AU,BZ,DZ,KP,KR,MZ,US

In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:

AE,AL,AM,AP,AT,AZ,BA,BB,BG,BR,BY,CA,CH,CN,CR,CU,CZ,DE,DK,DM,EA,EE,EP,ES,FI,GB,GD,  
GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,  
NO,NZ,OA,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZW

The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on 11 January 2001 (11.01.01) under No. WO 01/03100

## REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, a demand for international preliminary examination must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

## REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the national phase, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer J. Zahra
Facsimile No. (41-22) 740.14.35	Telephone No. (41-22) 338.83.38

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
11 January 2001 (11.01.2001)

PCT

(10) International Publication Number  
**WO 01/03100 A1**

(51) International Patent Classification<sup>7</sup>: **G08F 13/14**

(21) International Application Number: PCT/SE00/01407

(22) International Filing Date: 3 July 2000 (03.07.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
9902532-2 1 July 1999 (01.07.1999) SE

(71) Applicant (for all designated States except US): **SIKE & CO** [SE/SE]; Gjuterigatan 3 A, S-553 18 Jönköping (SE).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **GÜNDNER, Hans, Martin** [DE/DE]; Wartbergweg 1, D-71672 Marbach (DE). **LÖFFLER, Andreas** [DE/DE]; Grabbbruuneustr. 6,

73728 Esslingen (DE). **VEIT, Martin** [DE/DE]; Rosenst. 17, 72124 Pliezhausen (DE). **GUNNARSSON, Andreas** [SE/SE]; Sandbacksvägen 16A, S-553 16 Jönköping (SE). **FAHLÉN, Mattias** [SE/SE]; Vattugatan 5, S-172 73 Sundbyberg (SE).

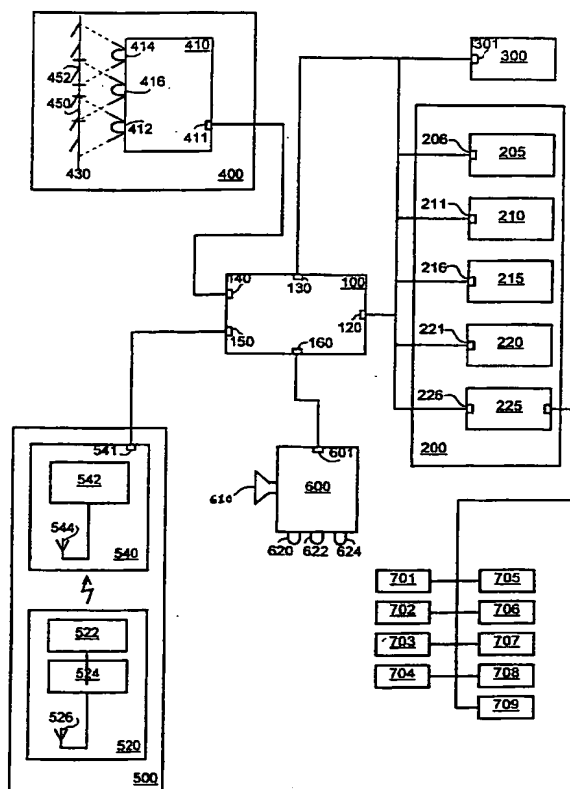
(74) Agent: **ALBIHNS PATENTBYRÅ STOCKHOLM AB**; Box 5581, S-114 85 Stockholm (SE).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: APPARATUS AND METHOD FOR SAFEGUARDING ELECTRONIC EQUIPMENT FROM THEFT



(57) Abstract: The present invention relates to an apparatus and a method for safeguarding valuable electronic equipment (701-709) from theft. The safeguarding apparatus is connected to a sensing means (400), monitoring whether an unauthorised person has opened a housing of the electronic equipment. An identification means identifies authorised users. Unauthorised breaking or opening of the housing results in activation of a destruction means (200) with an electric pulse fed through the electronic components (701-709), whereby said devices are irreversibly set out of order and thus their trade-in value is considerably diminished.

WO 01/03100 A1



IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

**Published:**

— *With international search report.*

## **Apparatus and method for safeguarding electronic equipment from theft**

### ***Technical field of the invention***

5     The invention relates to an apparatus and a method for preventing electronic equipment from theft.

### ***Background of the invention***

Current industrial as well as governmental and private investments in computerised equipment and electronic devices grow rapidly and these investments form property  
10     of considerable value to the owners. However, this valuable property also attracts people to commit criminal acts and in illegal ways get in possession of items belonging to others.

Not only the so-called hardware, i.e. interconnected electronic circuits with processing capacity, memories and displays, but also and perhaps even more vulnerable  
15     may be so-called software and content of various memory locations of, or in association with, the electronic devices. Occurrence of sensitive data or material stored in a memory location of e.g. a laptop computer in wrong hands may have severe consequences to any company, organisation or enterprise as well as to a private person if content stored in memory locations of the computer is made public, for what-  
20     ever reason.

Several mechanical means for prevention of computer thefts are offered on the market, especially for preventing people from stealing stationary desktop computers in offices. Those means may be for example metallic safety lockers or wires, which physically restrict people from opening or carrying the computer or its parts with  
25     them. Such physical means mostly are relatively expensive, cumbersome to install and not at all flexible. However, for mobile equipment like for instance portable

laptop computers, even less practical theft-preventing means are offered on the market, such as various attention attracting sirens and alarms. Most prior art safeguarding arrangements are software encryption systems, which for data protective reasons may be very useful although the electronic components do not lose their value after theft from the legitimate owner.

The UK patent application GB 2 304 810 A discloses a security arrangement with sensors detecting light levels inside of a personal computer housing or motion of the personal computer. Furthermore, the arrangement inside the computer consists of a dye capsule, which is intended to rupture and spray its content outwardly upon reception of an electrical signal. This signal is sent from an alarm output control when the personal computer is considered stolen. It is of course difficult to distinguish usual "every day" handling of the personal computer in reliable manners from unauthorised handling after the computer has been stolen. A clear disadvantage of an implemented security arrangement of that kind is the risk of numerous false alarms leading to strongly decreased acceptance of the arrangement.

The international patent application WO 97/03397 discloses a method and an arrangement for deterring computer-thefts by means of a protective device using detection with external sensors. Sensing is performed either by using a thin film with an electrically conductive film, or wall anchor plates mounted on a wall of the room in which the computer is used. It can also be performed by means of an external sensor disposed as an insert between the underside of the computer and the table surface on which the computer stands. However, a solution with a thin film conductive sensor suffers from the drawback, that the film will be destroyed each time the computer casing is opened, even when the casing is opened for normal service actions or for maintenance. This makes this method and arrangement less convenient as it requires restoration of the conductive thin film after having opened the computer casing in order to reach the original functional state again. A restoration of this kind is costly due to manual work required by professionals every time the computer casing has been opened.



***Summary of the invention***

An object of the present invention is to overcome the aforementioned drawbacks concerning prior art technology in connection with stationary and portable computers as well as with electronic devices and circuitry in general.

5 This object of the invention is accomplished by means of an apparatus for safeguarding electronic equipment, such as components in a computer, provided in a housing, comprising a monitoring internal sensor arrangement in connection with a control means, which is fed with measurement data to monitor whether the housing is closed or not,

10 characterised by

at least one energy provider, such as an internal or external power source;

voltage generating means, driven by power from the energy provider and controlled by the control means;

15 storage means, including a capacitor arrangement charged by the voltage generating means;

switching means, in connection with the storage means being adapted to be controlled by the control means; and

20 relayed connections between components of the the electronic equipment and the switching means, particularly chosen to get the electronic equipment irreversibly out of order when initiated by the control means in response to unauthorised opening of the housing.

A housing sensor means would be convenient, sensing if the housing is unauthorised opened, whereby the housing sensor means is adapted to send a warning signal  
25 to the control means, preferably a micro-controller, when sensing unauthorised opening. In another embodiment, a conceivable solution would be to use electronic equipment sensing means sensing unauthorised disconnection of at least one component in the electronic equipment, whereby the electronic equipment is adapted to

send an indication to the control means for activation of a destructive activation when detecting unauthorised disconnection.

The apparatus moreover comprises identification means, identifying a user and possibly authorising the user after comparison with a register, whereby the electronic equipment could be unlocked. Said identification means either comprises a so-called  
5 smart card reading means, operating with physical contacting or without physical contacting and/or a PIN-code reading means and/or any other human feature recognising means, such as a fingerprint and/or iris recogniser.

In order to guarantee provision of energy for running the safeguarding apparatus, an  
10 autonomous power supplying means such as a battery, preferably a rechargeable battery arrangement, may be provided, which is supplying the apparatus and its parts with the sufficient electric power after having been disconnected from a mains power outlet.

Suitably, said destruction means generates a pulse of high voltage and/or current,  
15 which is lead through the electronic circuitry, whereby essential components within the circuitry are irreversibly set out of order. Else, said destruction means could generate a destructive injection, preferably of a highly conductive, gluing and/or corroding chemical fluid, which is distributed over vulnerable and essential electronic components, whereby the components are irreversibly set out of order.

20 For enhanced flexibility, remote control means could be useful, by which remote signals from a remote control station can be received, and whereby actions can be taken by the safeguarding apparatus in response to sent remote signals.

Furthermore, prior art is afflicted with problems that are solved by a method for safeguarding electronic equipment, which electronic equipment is placed and pro-  
25 tected in a housing. The housing comprises monitoring means, such as an internal sensor arrangement, to monitor whether the housing is closed or not and/or whether an authorised person operates the electronic equipment. The method is characterised

by connecting and controlling the destruction initiation means by the monitoring means and providing at least one destruction means in the electronic equipment, which means has been particularly chosen to set the electronic equipment irreversibly of order when initiated by a destruction initiation means, such as a controlling micro-controller.

Owing to the present invention as here described, a novel approach is presented that offers the market a convenient and cheap apparatus and a method inhibiting incentives for stealing computer-related devices. The present invention has the advantage that the trade-in value of electronic devices, possibly removed from stolen computers is diminished due to the irreversible damage caused to the devices. It also constitutes a more flexible way of safeguarding electronic equipment, without limiting the mobility of the device, such as a stationary or portable computer.

### ***Brief description of the drawings***

The above and further features, advantages and benefits of the present invention will be apparent upon consideration of the following detailed description, taken in conjunction with the accompanying drawings, in which like reference characters and figures refer to like parts throughout, and in which:

Fig 1 shows a schematic overview of comprised units in a first embodiment of the safeguarding apparatus according to the present invention,

Fig 2 is a flow chart illustrating the sequence of activation, sensing, destruction and indication of operational states of the apparatus and the method here described.

### ***Detailed description***

The following description is of the best mode presently contemplated for practising the invention. The description is not to be taken in a limiting sense, but is made merely for the purpose of describing the general principles of the invention. The scope of the invention should be ascertained with reference to the issued claims.

With reference to Fig 1, a block diagram is shown of a first embodiment of the present invention for safeguarding electronic equipment like for instance a stationary or a portable computer. The main functional units of the apparatus according to the invention are mounted on a standard-sized slot card, preferably a so-called PCI-card adapted to be connectable to a corresponding PCI-slot within the computer casing, which is a slot format provided in most personal computers of today. Normally, the motherboard of a personal computer has a bi-directional connection 301 directly to an external power source 300 via a transformer (not shown here). According to this first embodiment, the external power source 300 is also connected via a transformer to the motherboard of the personal computer, but via a destruction means 200. There may also be direct connection between an input/output 130 of the micro-controller 130 and the external power source connection 301, but this optional. The destruction means 200 is provided on the PCI-card, and the destruction means 200 comprises a number of units, each of which has a certain functionality and is able to communicate bi-directionally with a micro-controller 100 via one of its inputs/outputs 120. The micro-controller 100 is in control of each action performed by the apparatus according to the invention including power management of the computer. The units of the destruction means 200 are the internal power management unit 205, a battery 210, preferably but not necessarily rechargeable, a voltage generating means 215, a capacitor arrangement 220, preferably including a plurality of capacitors connected in parallel, and finally a target component switch 225. Each one of the units of the destruction means 200 is connected to the micro-controller via inputs/outputs 206, 211, 216, 221 and 226 respectively.

Moreover, the micro-controller 100 communicates with a sensor means 400 via another of its inputs/outputs 140. The sensor means 400 is also mounted on the PCI-card, alternatively connected to it but attached in another position within the computer casing, and includes at least two main units. These main units are on one hand an IR-unit (infrared unit) 410 with an input/output 411 and on the other hand a reflective layer 430 attached to the inside of the casing of the personal computer. The

reflective layer 430 is preferably an adhesive, thin plastic film having stripes or another similar patterns or texture on it, with significant differences in contrast between its fields. Checkers as well as waved patterns are both conceivable for use in other embodiments of the present invention. The IR-unit 410 is mounted on the PCI-card in a way that a set of diodes including for instance three diodes 412, 414, 416 is directed perpendicularly towards the reflective layer 430. The set of diodes 412, 414, 416 is placed on the IR-unit 410 in a row, preferably with an IR-LED (infrared light emitting diode) 416 in the middle and one detecting photodiode 412, 414 on each side of the middle positioned IR-LED 416. Each of the diodes 412, 414, 416 has a non-transparent screening around it in order not to disturb or interfere with the other two diodes. This might occur in that undesired emission that has not been reflected from the reflective layer 430 or other undesired kinds of reflection, such as varying ambient light, would be captured by the detecting photodiodes 412, 414 instead of the properly reflected IR-light which is to be analysed.

The set of diodes 412, 414, 416 is arranged in a way that part of an emitted area and a detected area of the reflective layer will be overlapping. Two of these areas have been illustrated in Fig 1 and have been designated 450 and 452. The intensity of the reflected light energy of these areas 450, 452 is captured by the IR-unit 410 and measurement data on this reflected IR-light intensity is communicated to the micro-controller 100. A certain change in measurement value of the reflected IR-light intensity is a relevant indication that the casing of the computer has been moved, possibly for opening of the casing. Thus the micro-controller 100 is notified about the certain change and is able to respond to this relevant indication, perhaps by taking corresponding actions of for example initialising an irreversible destruction of certain components of the computer. Hence, the destruction mechanism will be activated before the casing is completely opened. Slow changes in the measured light energy, due to ambient temperature conditions, are detected and compensated by utilisation of a temperature sensor (not shown) in connection with the micro-controller 100.

Furthermore, and still with reference to Fig 1, a remote accessibility unit 500 is shown, by which unit 500 the safeguarding apparatus can be activated in a number of ways. The remote accessibility unit is connected to the micro-controller 100 via another of its inputs/outputs 150. The apparatus for irreversible destruction of stolen electronic equipment has four differently activated states of operation. To the user of for instance a personal computer, the safeguarding apparatus is either in a locked or unlocked state. The user herself/himself has a possibility of locking and unlocking the safeguarded computer, by means of a pocket-sized remote access transmitter 520, including at least one antenna 526, a RF-module (radio frequency module) 524 and a signal encoder 526, by which remote access transmitter 520 messages are encrypted, modulated and transmitted to the corresponding remote access receiver 540. Here they are received, demodulated and decoded, whereby software controlled by the micro-controller 100 is used for decoding the message. Transmission of data is performed in a standardised way over the air interface and the assigned radio frequency band for the customer products is utilised. The remote access receiver 540 is mounted on the PCI-card just like the other previously described units of the destruction means 200. The remote access receiver 540 also includes at least one antenna 544 and an RF-module 542. Except for the remote access transmitter 520, the antenna 544 of the remote access receiver 540 is the only part of the safeguarding arrangement that is not completely inside the computer casing. The antenna is protected by a cover and is coupled to the electric circuit through a capacitor, to prevent from external corruption of the apparatus, for instance by removing the cover and applying high-voltage to the antenna.

The locking and unlocking feature of the electronic equipment, in this embodiment a computer, is realised by redirecting the power switch to the micro-controller 100 and from there connecting to the motherboard of the computer. The connection between motherboard and micro-controller 100 enables checking whether the computer is connected to the external power source 300. The connection between the power switch and the micro-controller 100 enables turning on and turning off the

computer as well as to prevent powering of the computer, which here means to lock the computer.

For professionals, such as administrators or so-called super users, who are serving the computer or for maintenance reasons, it is possible to disarm the activation of the destruction mechanism prior to opening the casing of the computer to prevent  
5 undesired destruction of components. Subsequently, i.e. after having carried out technical services, replaced or updated components of the computer, the professional arms the destruction mechanism, whereby the computer is ready for use again. The various states armed/disarmed and locked/unlocked give rise to four different operational states of the computer, of which an ordinary user only accesses  
10 the lock and unlock features. Deactivation of the destruction functionality accessible exclusively for professionals, the mentioned administrators and super users.

Another main unit controlled by the micro-controller 100, via the input/output 160, is the user information unit 600. This unit visualises and notifies the user of the  
15 safeguarding apparatus about the present state of operation, i.e. armed/disarmed and locked/unlocked state. The user information unit 600 comprises a buzzer 610 for audio signals and at least one diode 620, 622, 624, preferably an LED, emitting visible light. Its is feasible to use visible LEDs of different visible colours and buzzer signals of different frequencies and volume for easy and unambiguous recognition of signal message, also by non-professional users with little technical inter-  
20 est and/or experience. Some of these diodes may be visible from the outside of the computer casing and others only from the inside. Hidden diodes inside the computer casing are to inform professionals when serving or maintaining the electronic equipment.

25 By means of the safeguarding apparatus of the present invention, a wide variety of components can be irreversibly destructed. In a first embodiment of the invention, destruction of components is obtained by means of transferring a built-up voltage from the loaded capacitor arrangement 220 via the target component switch 225. In

most cases, the rather low level of voltage is applied, approximately as low voltage as 20-40 V, in the opposite direction relative to the usual voltage direction when a component is in a normal state of operation. By applying the voltage in the opposite direction, a rectifier or another type of diode may be broken, whereby the component to be destructed is easily accessible. Some of the valuable components of the computer that can be irreversibly destructed by means of the apparatus are the following: non-volatile memory locations like the hard disk 701 and other disks 702, the motherboard 703 and the central processing unit 704. Also various expansion cards 705 like the graphic card, video card, audio card and network card can be destructed. Other units that are included among components to be destructed are the DVD- 706 and/or CD player 707. In addition to the previously mentioned components, also read only memories 708, flash memories 709, etc, are included. Each valuable and theft-attractive component is safeguarded and can be destructed by means of the apparatus according to the present invention.

A delicate task, which is of crucial importance in a safeguarding apparatus like the present invention, is to prevent undesired destruction of computer components due to unexpected or unwanted events taking place. A single error in a logical signal could, in a worst case scenario, lead to irreversible destruction of all electronic components in a computer. Logical signal errors may occur in all kinds of electronic equipment, so the consequences must not be of the previously mentioned critical nature. The present invention solves the problem in two ways. The voltage used for destruction is generated by a circuitry including a transformer, a rectifier and a load capacitor. Generation of a relatively low level of voltage, which still is sufficient for destruction of components 701-709, can be accomplished by the voltage generating means 215 in a short period of time in comparison to high-voltage levels. According to measurements only a period of a few tenths of a second is required for reaching a voltage level in the capacitor arrangement 220 of about 30 V. Loading of the capacitor arrangement 220 is initiated first when the micro-controller 100 decides to take actions for destruction of components. However, the alternating input voltage is



not generated in usual manners by a distinct oscillating circuit, but by means of the micro-controller 100. The alternating output voltage is produced on one of the output pins of the micro-controller 100 and thus, the alternating output voltage is controlled by software. An erroneous logical signal can not trigger the destruction mechanism of the destruction means 200 unless the required voltage level of the capacitor arrangement 220 has been generated at first. If the either hardware or software of the micro-controller 100 for whatever reason would fail, no alternating signal is produced and hence no voltage will be built-up. Therefore, the destruction mechanism is intrinsically safe and will not ever be activated by mistake.

Another additional safety arrangement, which is achieved by the circuitry design, is that the activation of the destructive capacitor arrangement voltage is performed by the micro-controller 100. This means that even if a voltage has been built-up and is about to be lead on to destruction of electronic components, it does not have to be switched out to the components 701-709 via the target component switch 225. This switching is controlled and performed by the micro-controller 100, whereby activation by mistake will not ever occur in case voltage for destruction already has been built up.

Although the shifts between operational states of the safeguarding apparatus in a first embodiment are made by means of the previously described encoding radio frequency key 520, there are many other conceivable methods for identification and authentication of users. Another way of shifting between operational states, such as unlocking and disarming, is by means of identification procedures, such as using a smart card or manual keying of a PIN-code by an operator or user. When identification is accomplished, the operator or user candidate is compared with a register of predefined authorised operators or users and the candidate may subsequently be authorised for usage of safeguarded electronic equipment. The identification process could also take advantage of any other unique human features and it is conceivable to utilise fingerprint recognition or iris detection techniques.

Moreover, to the function of the destruction means 200, the voltage generating means 215 generates one for the electric circuitry excessively high voltage and/or current, which passes the target component switch 225, and is lead through the circuitry. Preferably it is lead as a reverse current through a diode, whereby essential electronic devices either melt or are otherwise irreversibly damaged and made use-  
5 less. In another embodiment, destructive highly conductive or corrosive chemical fluid is stored in the vicinity of sensitive the electronic components. At absolute and definite control from the micro-controller 100, the fluid may be set free and can thus be distributed over essential and vulnerable components 701-709 to be safeguarded,  
10 and eventually destructed, in the computer. Hereby is achieved a similar way of destruction of essential components either through short-circuiting electrical circuitry or corroding vital components instead of melting as in the first embodiment. Also a combination of the above-mentioned techniques is a feasible and effective way, in which the safeguarding apparatus works.

15 Except for the locking and unlocking radio frequency key, called the remote access transmitter 520, it is possible to use other wireless interfaced transceiver means. Such means could be a mobile telephone, a PDA and/or a variety of infrared communication terminals, each one of them enabling a way of remote accessibility to the safeguarding apparatus as well as authenticating and identifying the operator or  
20 user of the safeguarding apparatus.

Next reference is to Fig 2, which is a flow chart sequentially showing the steps for irreversible destruction of electronic components contained in the computer. Depending on the access rights of the current user or professional, the here used terms activate and inactivate should be changed to lock and unlock. The sequence starts  
25 (step 900) with a choice of whether the destruction means 200 is activated (step 901) or not. In case it is not activated, the sequence proceeds with the user's option to activate (step 902) the destruction means 200. If the user decides not to activate it, the sequence ends (step 915), otherwise the destruction means 200 is activated (step 903). In response to this activation, the user information unit 600 indicates

(904) the change in operational state to the user. In case the destruction means already was activated, or currently has become, the sequence follows up with an ongoing analysis (step 905) of the signals transmitted from the sensor means 400. Either, the sensor means 400 is polled by the micro-controller 100, or the sensor means 400 continuously updates the micro-controller 100 about current measurement data. As soon as the computer casing is opened (step 906), the micro-controller 100 is notified about it and has the responsibility for taking further action in response to the indication. As long as the computer casing remains closed, the user has an option to inactivate (step 907) the destruction means 200, for example by locking it. If the user decides to, the destruction means 200 is inactivated (step 908) and proceeds to the end (step 915) of the sequence, otherwise the micro-controller 100 instructs comprised units to continue analysing (step 905) the sensor signals received.

However, if an opening (step 906) of the computer casing is unambiguously detected by the micro-controller 100 and hence a destructive action is to be taken, the micro-controller 100 finds out whether the capacitor arrangement 220 is sufficiently charged (step 909) for enabling the destruction of components. In case it is not, the micro-controller 100 instructs the voltage generating means 215 to charge (step 910) the capacitor arrangement 220 until it has reached a sufficient level of charge. As soon as the sufficient level of charge is reached, the micro-controller 100 instructs the destruction means to destruct (step 911) a first component. As long as any component remains functional (step 912), or has not yet been completely and irreversibly destructed, the target component switch 225 of the destruction means 200 switches (step 913) the focus of destruction to another target component to destruct. When there is no more functional component remaining, the user information unit 600 informs the user about this by indicating (step 914) the destructed state of operation. Hence, the sequence has reached its end (step 915).

## Claims

1. An apparatus for safeguarding electronic equipment, such as components (701-709) in a computer, provided in a housing, comprising a monitoring internal sensor arrangement (400) in connection with a control means (100), which is fed with measurement data to monitor whether the housing is closed or not,

**characterised by**

at least one energy provider (205, 210, 300), such as an internal or external power source;

voltage generating means (215), driven by power from the energy provider (205, 210, 300) and controlled by the control means (100);

storage means (220), including a capacitor arrangement charged by the voltage generating means (215);

switching means (225), in connection with the storage means (220) being adapted to be controlled by the control means (100); and

relayed connections between components (701-709) of the electronic equipment and the switching means (225), particularly chosen to get the electronic equipment irreversibly out of order when initiated by the control means (100) in response to unauthorised opening of the housing.

2. An apparatus according to claim 1, **characterised by**

remote accessibility unit (500) in connection with the micro-controller (100) to feed an air-interfaced signal controlling the operational state of the safeguarding apparatus remote control.

3. An apparatus according to claim 1 or 2, **characterised by**

housing sensor means (400) sensing if the housing is unauthorised opened, whereby the housing sensor means (200) is adapted to transmit an indication to the micro-controller (100) when the housing is opened.

4. An apparatus according to anyone of the claims 1-3, **characterised by**  
electronic equipment sensing means (400) sensing unauthorised dis-  
connection of at least one component of the electronic equipment (701-709),  
whereby the electronic equipment (100) is adapted to send a warning signal to  
5 the micro-controller (100) when detecting unauthorised disconnection.
5. An apparatus according to anyone of the preceding claims, **characterised by**  
identification means, identifying a user and possibly authorising the op-  
erator or user after comparison with a register, whereby the electronic equipment  
is unlocked.
- 10 6. An apparatus according to claim 5, **characterised in that**  
said identification means either is a so-called smart card reading means,  
operating with physical contacting or without physical contacting or a PIN-code  
reading means or any other human feature recognising means, such as a finger-  
print and/or iris recogniser.
- 15 7. An apparatus according to anyone of the claims 1-4, **characterised in that**  
said energy provider (205, 210) is an autonomous power supplying  
means (210), such as a battery, supplying the apparatus with electric power after  
having been disconnected from an external power source (300).
- 20 8. An apparatus according to anyone of the claims 1-4, **characterised in that**  
voltage generating means (215) generates voltage and/or current, which  
is lead through electronic circuitry, whereby essential electronic components  
within the circuitry are irreversibly set out of order.
- 25 9. An apparatus according to anyone of the claims 1-4, **characterised in that**  
a destruction means (200) is adapted to generate a destructive injection,  
preferably of a highly conductive and/or corroding chemical fluid, which is dis-  
tributed over essential electronic components, whereby the components are irre-  
versibly set out of order.

10. An apparatus according to anyone of the claims 1-4, **characterised by**

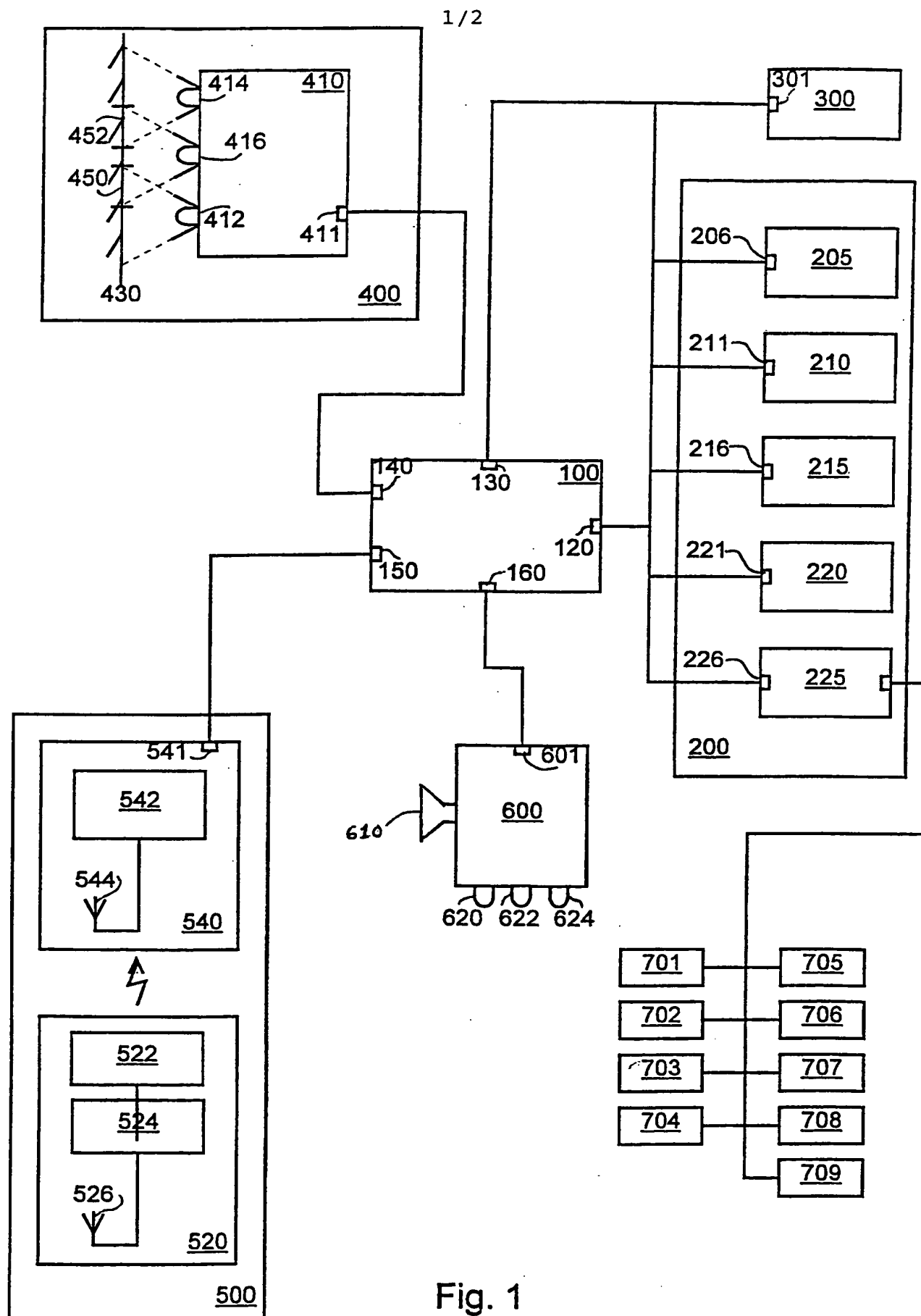
remote receiving control means (540), by which transmitted remote signals from a remote transmitting control means (520) are received, adapted to take actions in response to instructions given by the micro-controller (100).

5 11. A method of safeguarding electronic equipment (701-709) provided in a housing, comprising monitoring internal sensor arrangement (400) in connection with a control means (100), to monitor whether the housing is closed or not and/or whether the electronic equipment is operated by an authorised person, **characterised by**

10 controlling a destruction means (200) by the control means (100), preferably by a micro-controller (100);

providing the control means (100) with indications from a sensor means (400) for activating the destruction means (200), particularly chosen to set electronic components (701-709) irreversibly out of order when initiated by the control means (100).

15



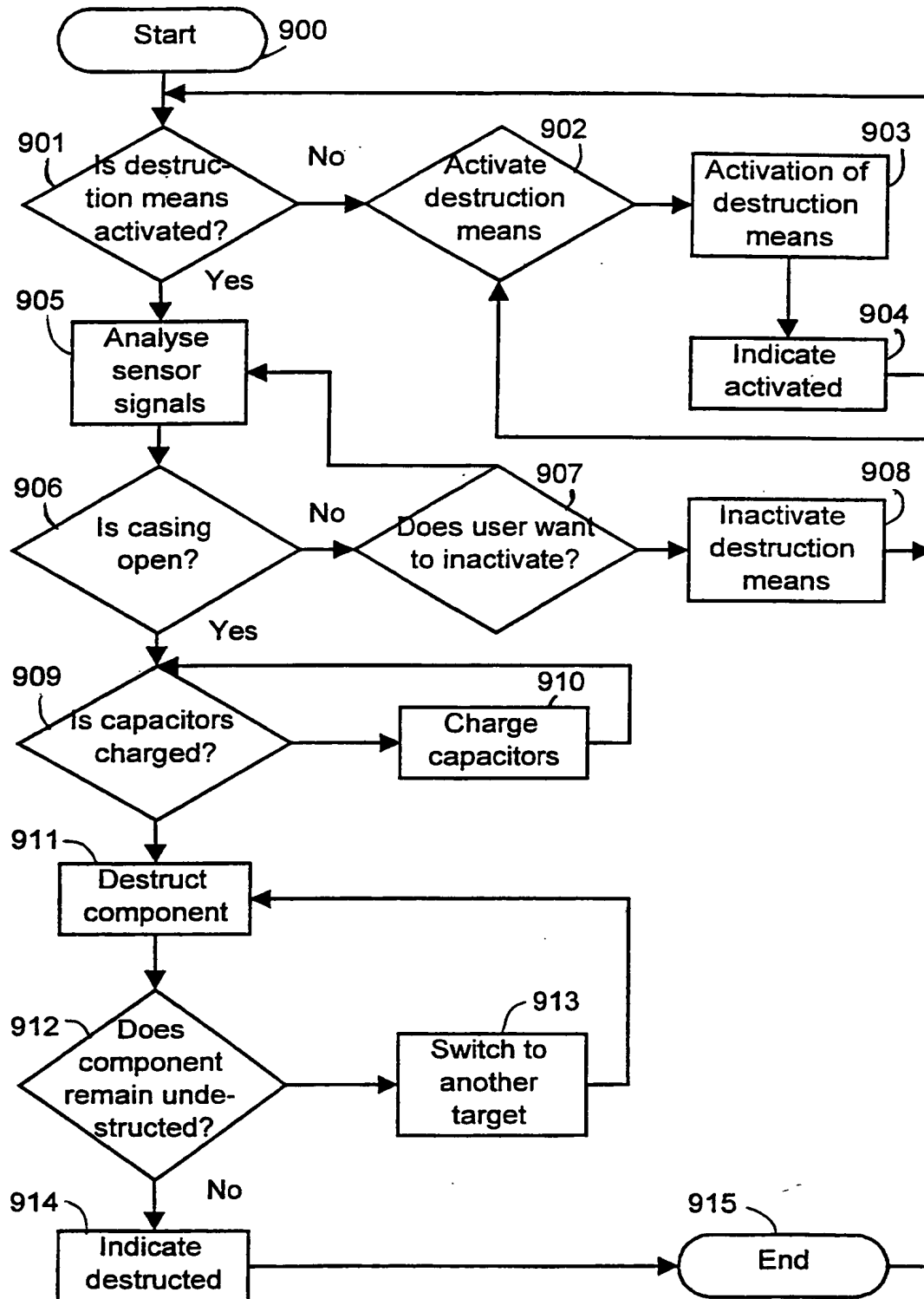


Fig. 2



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 00/01407

## A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G08F 13/14

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G08B, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9703397 A1 (BENKTA CONSULTING AB), 30 January 1997 (30.01.97), page 1, line 34 - page 2, line 17; page 3, line 7 - page 4, line 16	1,3-8,11
Y	--	2,9
X	US 5406261 A (J.T.GLENN), 11 April 1995 (11.04.95), column 4, line 16 - line 36; column 5, line 50 - column 6, line 7; column 7, line 21 - line 47, figures 4,5	11
Y	--	2,9

☒ Further documents are listed in the continuation of Box C.☒ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&amp;" document member of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report

7 October 2000

17-10-2000

Name and mailing address of the ISA/

Swedish Patent Office

Box 5055, S-102 42 STOCKHOLM

Facsimile No. +46 8 666 02 86

Authorized officer

Gunnel Wästerlid/itw

Telephone No. +46 8 782 25 00

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 00/01407

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5767771 A (L.A.LAMONT), 16 June 1998 (16.06.98), column 3, line 40 - column 4, line 57; column 5, line 29 - line 52, figure 6  --	1,3-8,11
Y	GB 2300508 A (DERITEND ELECTRO-MECHANICAL SERVICES LTD.), 16 November 1996 (16.11.96), page 1, line 38 - page 2, line 14; page 4, line 28 - page 5, line 21; page 6, line 4 - line 21, abstract, p.7,1.5-p.8,1.12,p.9, 1.26-1.33  --	1,3-8,11
A	US 5760690 A (R.A.FRENCH), 2 June 1998 (02.06.98), column 1, line 57 - column 2, line 21  -- -----	1-11

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

01/08/00

International application No.  
PCT/SE 00/01407

Patent document cited in search report			Publication date	Patent family member(s)	Publication date
WO	9703397	A1	30/01/97	SE 9502537 A	11/01/97
US	5406261	A	11/04/95	NONE	
US	5767771	A	16/06/98	NONE	
GB	2300508	A	16/11/96	AU 2529495 A	21/11/96
				GB 2300743 A	13/11/96
				GB 9508716 D	00/00/00
				GB 9514679 D	00/00/00
				WO 9635195 A	07/11/96
US	5760690	A	02/06/98	NONE	

REVISED VERSION

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
11 January 2001 (11.01.2001)

PCT

(10) International Publication Number  
**WO 01/03100 A1**

(51) International Patent Classification<sup>7</sup>: **G08B 13/14**

(21) International Application Number: **PCT/SE00/01407**

(22) International Filing Date: **3 July 2000 (03.07.2000)**

(25) Filing Language: **English**

(26) Publication Language: **English**

(30) Priority Data:  
**9902532-2** **1 July 1999 (01.07.1999)** **SE**

(71) Applicant (for all designated States except US): **SIKE & CO [SE/SE]; Gjuterigatan 3 A, S-553 18 Jönköping (SE).**

(72) Inventors; and

(75) Inventors/Applicants (for US only): **GÜNDNER, Hans, Martin [DE/DE]; Wartbergweg 1, D-71672 Marbach (DE). LÖFFLER, Andreas [DE/DE]; Grabbruuneustr. 6, 73728 Esslingen (DE). VEIT, Martin [DE/DE]; Rosenst.**

**17, 72124 Pliezhausen (DE). GUNNARSSON, Andreas [SE/SE]; Sandbacksvägen 16A, S-553 16 Jönköping (SE). FAHLÉN, Mattias [SE/SE]; Vattugatan 5, S-172 73 Sundbyberg (SE).**

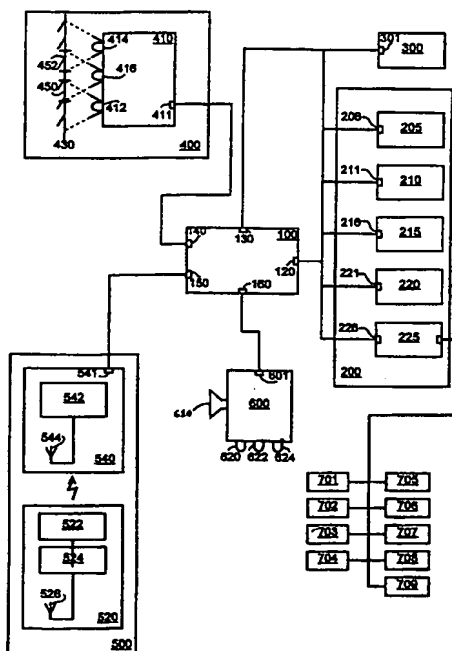
(74) Agent: **ALBIHNS PATENTBYRA STOCKHOLM AB; Box 5581, 114 85 Stockholm (SE).**

(81) Designated States (national): **AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.**

(84) Designated States (regional): **ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,**

[Continued on next page]

(54) Title: **APPARATUS AND METHOD FOR SAFEGUARDING ELECTRONIC EQUIPMENT FROM THEFT**



(57) Abstract: The present invention relates to an apparatus and a method for safeguarding valuable electronic equipment (701-709) from theft. The safeguarding apparatus is connected to a sensing means (400), monitoring whether an unauthorised person has opened a housing of the electronic equipment. An identification means identifies authorised users. Unauthorised breaking or opening of the housing results in activation of a destruction means (200) with an electric pulse fed through the electronic components (701-709), whereby said devices are irreversibly set out of order and thus their trade-in value is considerably diminished.

WO 01/03100 A1



IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**(15) Information about Correction:**

see PCT Gazette No. 19/2001 of 10 May 2001, Section II

**Published:**

— *With international search report.*

**(88) Date of publication of the revised international search report:**  
10 May 2001

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 00/01407

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G08B 13/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G08B, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9703397 A1 (BENKTA CONSULTING AB), 30 January 1997 (30.01.97), page 1, line 34 - page 2, line 17; page 3, line 7 - page 4, line 16	1,3-8,11
Y	--	2,9
X	US 5406261 A (J.T.GLENN), 11 April 1995 (11.04.95), column 4, line 16 - line 36; column 5, line 50 - column 6, line 7; column 7, line 21 - line 47, figures 4,5	11
Y	--	2,9

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 16.02.2001	Date of mailing of the international search report 20-02-2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Gunnel Wästerlid/itw Telephone No. +46 8 782 25 00

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 00/01407

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5767771 A (L.A.LAMONT), 16 June 1998 (16.06.98), column 3, line 40 - column 4, line 57; column 5, line 29 - line 52, figure 6  --	1,3-8,11
Y	GB 2300508 A (DERITEND ELECTRO-MECHANICAL SERVICES LTD.), 16 November 1996 (16.11.96), page 1, line 38 - page 2, line 14; page 4, line 28 - page 5, line 21; page 6, line 4 - line 21, abstract, p.7,1.5-p.8,1.12,p.9, 1.26-1.33  --	1,3-8,11
A	US 5760690 A (R.A.FRENCH), 2 June 1998 (02.06.98), column 1, line 57 - column 2, line 21  -- -----	1-11

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

01/08/00

International application No.

PCT/SE 00/01407

Patent document cited in search report			Publication date	Patent family member(s)		Publication date
WO	9703397	A1	30/01/97	SE	9502537 A	11/01/97
US	5406261	A	11/04/95	NONE		
US	5767771	A	16/06/98	NONE		
GB	2300508	A	16/11/96	AU	2529495 A	21/11/96
				GB	2300743 A	13/11/96
				GB	9508716 D	00/00/00
				GB	9514679 D	00/00/00
				WO	9635195 A	07/11/96
US	5760690	A	02/06/98	NONE		



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**